UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/757,872	01/10/2001	John S. Flowers	22192-06893	8233

758 7590 03/30/2006

FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
TRAN, ELLEN C	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 03/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/757,872	FLOWERS ET AL.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *30-55* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *30-55* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *AUG'05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. In response to amendment filed on 11 October 2005, the original application was filed on 10 January 2001 with a continuing application priority date of 10 January 2000.

2. Claims 30-55 are currently pending. Claims 1-29 have been cancelled by amendment, claims 30-55 are new. Amendments to the claims are accepted.

Response to Arguments

3. Applicant's arguments with respect to 30-55 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 30-55 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The non-statutory subject matter is the abstract idea that does not have a practical application because the 'vulnerability or intrusion detection rules' are always changing in addition the conditions for detecting an intrusion or vulnerability situation are not constant. If the applicant is attempting to define the rule based on associated conditions (and according to claim 31 automatically, without human intervention, arguments submitted 6 December 2004, page 9) a significant amount of detail needs to be added to the claims, and the rule has to be given a constant set of parameters. The idea of: providing or generating or determining rules based on a condition of the rule (which is being provided, generated, or determined) do not provide concrete repeatable results and therefore are not patentable. The

claim steps have to indicate how the rule is defined, one cannot define the rule based on something that is not yet defined.

In formulating this 101 rejection the examiner does not find that the claims transform the article, i.e. the computer is not changed. Therefore the examiner reviewed the claims to determine if the claims provide a practical application that produces a useful, tangible and concrete result. Of these three tests the examiner finds the claims fail the tangible and concrete result test.

In determining whether the claim is for a "practical application," the focus is not on whether the steps taken to achieve a particular result are useful, tangible and concrete, but rather that the final result achieved by the claimed invention is "useful, tangible and concrete."

In determining whether a claim provides a practical application that produces a useful, tangible, and concrete result, the examiner finds the claim are not a "TANGIBLE RESULT"

The tangible requirement does not necessarily mean that a claim must either be tied to a particular machine or apparatus or must operate to change articles or materials to a different state or thing. However, the tangible requirement does require that the claim must recite more than a § 101 judicial exception, in that the process claim must set forth a practical application of that § 101 judicial exception to produce a real-world result. The claims do not produce a real-world result because they are trying to provide rules based on conditions that occur in the future and that have not been previously defined.

In determining whether a claim provides a practical application that produces a useful, tangible, and concrete result, the examiner finds the claims are not a "CONCRETE RESULT".

Another consideration is whether the invention produces a "concrete" result. Usually, this question arises when a result cannot be assured. In other words, the process must have a result that can be substantially repeatable or the process must substantially produce the same result again. In re Swartz, 232 F.3d 862, 864, 56 USPQ2d 1703, 1704 (Fed. Cir. 2000) (where asserted result produced by the claimed invention is "irreproducible" claim should be rejected under section 101). The opposite of "concrete" is unrepeatable or unpredictable. Resolving this question is dependent on the level of skill in the art. For example, if the claimed invention is for a process which requires a particular skill, to determine whether that process is substantially repeatable will necessarily require a determination of the level of skill of the ordinary artisan in that field. Because intrusion methods are always changing the rules to detect intrusions are changing. Therefore the claimed invention is not concrete.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 30-55 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The vulnerability detection rules and the intrusion detection rules claimed are not concrete as noted above, therefore the claims due not meet the enablement requirement.

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 30-55 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

All claims contain text as noted above where the rules are provided based on a condition that meets the rule to be provided; this is abstract and therefore indefinite.

10. To expedite a complete examination of the instant application the claims rejected under 35 U.S.C. 101 (nonstatutory) as well as 35 U.S.C. 112 above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

12. Claims 1-10 and 13-29, are rejected under 35 U.S.C. 102(a) as being anticipated by Freund U.S. Patent No. 5,987,611 (hereinafter '611).

As to independent claim 30, "A computer-implemented method for use on a network to analyze a network resource from a remote location, comprising:" is taught in '611 col. 5, lines 12-15;

"providing vulnerability detection rules for determining at least one of an application and an operating system on the network resource, and for selecting vulnerabilities associated with the at least one of the determined application and the determined operating system" is shown in '611 col. 3, lines 60-65;

"based on responses from the network resource satisfying conditions of the vulnerability detection rules; and" is disclosed in '611 col. 4, lines 23-28;

"providing intrusion detection rules, corresponding to the selected vulnerabilities, for examining network traffic for attacks on the at least one of the determined application and the determined operating system responsive to the network traffic satisfying conditions of the intrusion detection rules" is taught in '611 col. 4, lines 51-63.

As to dependent claim 31, "further comprising: detecting the at least one of the application and the operating system, wherein the intrusion detection rules are automatically provided upon detection" is shown in '611 col. 5, lines 44-64 (note automatically would be the case when the process is prevented from access the Internet).

As to independent claim 32, "A method for use on a network to analyze a network resource from a remote location, comprising" is taught in '611 col. 5, lines 12-15;

"providing vulnerability detection rules for determining at least one of an application and an operating system on the network resource, and for selecting vulnerabilities associated with the at least one of the determined application and the determined operating system" is shown in '611 col. 3, lines 60-65;

"based on responses from the network resource satisfying conditions of the vulnerability detection rules" is disclosed in '611 col. 4, lines 23-28.

As to dependent claim 33, "wherein the responses from the network resources comprise reflex signatures indicative of the at least one of the determined application and the determined operating system" is disclosed in '611 col. 9, lines 14-16 (note the 'reflex signatures' are interpreted to be equivalent to 'filtering incoming data ... for detecting viruses or Trojan Horse programs').

As to dependent claim 34, "further comprising: prior to providing the vulnerability detection rules, generating templates to associate vulnerabilities with applications and operating systems, wherein a vulnerability detection rule selecting vulnerabilities selects a template corresponding to the determined application or the determined operating system" is taught in '611 col. 22, line 44 through col. 23, line 23 (note the template is interpreted to have the same meaning as the GUI displayed in FIG 6A through 7K).

As to dependent claim 35, "wherein a vulnerability detection rule comprises a complex rule that establishes logical relationships between two or more templates, and wherein a vulnerability detection rule selecting vulnerabilities selects the two or more templates" is shown in '611 col. 22, line 44 through col. 23, line 23.

As to dependent claim 36, "further comprising: providing vulnerability detection rules for detecting the network resource on the network, and for selecting vulnerabilities associated with network resources having any operating system" is disclosed in '611 col. 7, lines 12-30.

As to dependent claim 37, "further comprising: providing vulnerability detection rules for detecting a specific open port on the network resource, and for selecting vulnerabilities associated with the specific open port" is taught in '611 col. 19, lines 44-50.

As to dependent claim 38, "wherein a vulnerability detection rule determining at least one of the determined application and the determined operating system on the network resource comprises a challenge-response test to send data to the network resource and elicit a response indicative of the a least one of the determined application and the determined operating system" is shown in '611 col. 28, lines 55-67 .

As to dependent claim 39, "wherein the determined application comprises one or more from the group containing: tcmmux, echo, netstat, ftp, telnet and a network service" is disclosed in '611 col. 4, line 64 through col. 5, line 5.

As to dependent claim 40, "further comprising: providing intrusion detection rules for examining network traffic responsive to the selected vulnerabilities" is taught in '611 col. 9, lines 9-13.

As to dependent claim 41, "wherein intrusion detection rules for examining network traffic examine one or more fields of a network packet for predetermined values indicative of the selected vulnerabilities" is shown in '611 col. 11, line 36 through col. 13, line 56 (note 'examining the network packet' is interpreted to have the same meaning as 'intercepting and interpreting all TCP/IP communication').

As to dependent claim 42, "wherein intrusion detection rules detects an attack on the selected vulnerabilities responsive the network traffic satisfying conditions of the intrusion detection rules" is disclosed in '611 '611 col. 4, lines 23-28.

As to independent claim 43, this claim is directed to a device with a database to store the method of claim 30; therefore it is rejected along similar rationale.

As to dependent claim 44, this claim is substantially similar to claim 31; therefore it is rejected along similar rationale.

As to independent claim 45, this claim is directed to a device that implants the method of claim 32; therefore it is rejected along similar rationale.

As to dependent claims 46-55, these claims contain substantially similar subject matter as claims 33-42; therefore they are rejected along similar rationale.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 2:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques H. Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ECT

Ellen. Tran
Patent Examiner
Technology Center 2134
26 March 2006